



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/017,309	12/14/2001	Dieter Ansel	4283	7230
21553	7590	07/12/2005	EXAMINER	
FASSE PATENT ATTORNEYS, P.A.				TAYLOR, BARRY W
P.O. BOX 726				ART UNIT
HAMPDEN, ME 04444-0726				PAPER NUMBER
				2643

DATE MAILED: 07/12/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/017,309	ANSEL, DIETER	
	Examiner	Art Unit	
	Barry W. Taylor	2643	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 07 March 2005.
- 2a) This action is FINAL. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-4, 7 and 10-25 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 1-4, 7 and 10-25 is/are rejected.
- 7) Claim(s) _____ is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on 14 December 2001 is/are: a) accepted or b) objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) All b) Some * c) None of:
1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date: _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date: _____ | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

1. Claims 1-4, 7 and 10-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Groger (6,825,774) in view of Khello (5,724,423).

Regarding claim 1. Groger teaches a contactless data transmission system (see figure 1) with an encoding algorithm in which (item 27 figure 1, col. 2 lines 50-64) the input data (items 28 figure 1), which are processed with the encoding algorithm (see col. 2 lines 10-64 wherein the input data are encrypted), wherein the data transmission system has a facility (see one or more operating elements 28 figure 1, see button pressed---col. 3 lines 37-60) for setting to different formats of the input data for the encoding algorithm.

Groger does not explicitly show setting the encryption algorithm to different input word lengths.

Khello teaches a method and apparatus for user authentication wherein user selects code length (abstract, col. 10 lines 9-38) to provide different levels of security (abstract, col. 2 lines 46-49, col. 2 line 63 – col. 4 line 55, col. 8 lines 4-26). Khellos further discloses that the code length may be determined automatically by CPU or

manually by person (col. 9 lines 24-53) providing an encryption algorithm that is highly secure against eavesdroppers.

Therefore, it would have been obvious for any one of ordinary skill in the art at the time of invention to modify the code generator (i.e. item 27 figure1) as taught by Groger to incorporate the variable code length as taught by Khello for the benefit of providing a more secure system in that it allows the user to select different levels of security.

Regarding claim 2. Groger further shows using control line (see control line connecting item 25 and 27 in figure 1).

Regarding claim 3. Groger further shows using switches (item 28 figure 1) to select different types of formats (col. 3 lines 50-60).

Regarding claim 4. Groger teaches the same algorithm used but is silent with respect to various input word lengths.

Khello teaches a method and apparatus for user authentication wherein user selects code length (abstract, col. 10 lines 9-38) to provide different levels of security (abstract, col. 2 lines 46-49, col. 2 line 63 – col. 4 line 55, col. 8 lines 4-26). Khellos further discloses that the code length may be determined automatically by CPU or manually by person (col. 9 lines 24-53) providing an encryption algorithm that is highly secure against eavesdroppers.

Therefore, it would have been obvious for any one of ordinary skill in the art at the time of invention to modify the code generator (i.e. item 27 figure1) as taught by

Art Unit: 2643

Groger to incorporate the variable code length as taught by Khello for the benefit of providing a more secure system in that it allows the user to select different levels of security.

Regarding claims 7 and 10. Groger teaches the same code used but is silent with respect various input word lengths.

Khello teaches a method and apparatus for user authentication wherein user selects code length (abstract, col. 10 lines 9-38) to provide different levels of security (abstract, col. 2 lines 46-49, col. 2 line 63 – col. 4 line 55, col. 8 lines 4-26). Khellos further discloses that the code length may be determined automatically by CPU or manually by person (col. 9 lines 24-53) providing an encryption algorithm that is highly secure against eavesdroppers.

Therefore, it would have been obvious for any one of ordinary skill in the art at the time of invention to modify the code generator (i.e. item 27 figure1) as taught by Groger to incorporate the variable code length as taught by Khello for the benefit of providing a more secure system in that it allows the user to select different levels of security.

Regarding claim 11. Groger teaches a data transmission system adapted to carry out a contactless encrypted data transmission, comprising a first device (see item 10 or 20 figure 1) and a second device (see item 10 or 20 figure 1), wherein one of

devices (see item 20 figure 1) further includes an encryption unit (col. 2 lines 10-64, col. 3 lines 37-60).

Groger does not explicitly show the encryption unit adapted to receive a plural different input data respectively having different input data word lengths.

Khello teaches a method and apparatus for user authentication wherein user selects code length (abstract, col. 10 lines 9-38) to provide different levels of security (abstract, col. 2 lines 46-49, col. 2 line 63 – col. 4 line 55, col. 8 lines 4-26). Khellos further discloses that the code length may be determined automatically by CPU or manually by person (col. 9 lines 24-53) providing an encryption algorithm that is highly secure against eavesdroppers.

Therefore, it would have been obvious for any one of ordinary skill in the art at the time of invention to modify the code generator (i.e. item 27 figure1) as taught by Groger to incorporate the variable code length as taught by Khello for the benefit of providing a more secure system in that it allows the user to select different levels of security.

Regarding claim 12. Groger further shows using switches (item 28 figure 1) to select different types of formats (col. 3 lines 50-60).

Regarding claim 13. Groger further shows using control line (see control line connecting item 25 and 27 in figure 1).

Regarding claim 14. Groger does not elaborate on the size of encryption algorithm used with respect to the number of "bits". Khellos allows the user or CPU to

Art Unit: 2643

select size of code word to provide different levels of security (see rejection listed for claim 11 directly above). Therefore, using 32 bits for lower security and 64 bits for higher security would have been an obvious measure to one of ordinary skill in the art at the time of invention.

Regarding claim 15. Groger does not elaborate on the size of the algorithm used with respect to "short" or "long". Khellos allows the user or CPU to select size of code word to provide different levels of security (see rejection listed for claim 11 directly above). Therefore, using smaller (i.e. short) word lengths for lower security and larger (i.e. long) word lengths for higher security would have been an obvious measure to one of ordinary skill in the art at the time of invention.

Regarding claim 16. Groger does not teach different output word lengths being used.

Khellos teaches a method and apparatus for user authentication wherein user selects code length (abstract, col. 10 lines 9-38) to provide different levels of security (abstract, col. 2 lines 46-49, col. 2 line 63 – col. 4 line 55, col. 8 lines 4-26). Khellos further discloses that the code length may be determined automatically by CPU or manually by person (col. 9 lines 24-53) providing an encryption algorithm that is highly secure against eavesdroppers.

Therefore, it would have been obvious for any one of ordinary skill in the art at the time of invention to modify the code generator (i.e. item 27 figure1) as taught by Groger to incorporate the variable code length as taught by Khellos for the benefit of

providing a more secure system in that it allows the user to select different levels of security.

Regarding claim 17. Applicant's have already acknowledged that Groger uses fixed length (i.e. a specified consistent result word length, see paper dated 3/7/05, second to last paragraph on page 18) but is silent with respect to using different input data word lengths.

KhHello teaches a method and apparatus for user authentication wherein user selects code length (abstract, col. 10 lines 9-38) to provide different levels of security (abstract, col. 2 lines 46-49, col. 2 line 63 – col. 4 line 55, col. 8 lines 4-26). KhHello further discloses that the code length may be determined automatically by CPU or manually by person (col. 9 lines 24-53) providing an encryption algorithm that is highly secure against eavesdroppers.

Therefore, it would have been obvious for any one of ordinary skill in the art at the time of invention to modify the code generator (i.e. item 27 figure1) as taught by Groger to incorporate the variable code length as taught by KhHello for the benefit of providing a more secure system in that it allows the user to select different levels of security.

Method claim 18 is rejected for the same reasons as system claim 11 since the recited elements would perform the recited method steps.

Regarding claim 19. Groger does not explicitly show input data having different word lengths.

KhHello teaches a method and apparatus for user authentication wherein user selects code length (abstract, col. 10 lines 9-38) to provide different levels of security (abstract, col. 2 lines 46-49, col. 2 line 63 – col. 4 line 55, col. 8 lines 4-26). KhHello further discloses that the code length may be determined automatically by CPU or manually by person (col. 9 lines 24-53) providing an encryption algorithm that is highly secure against eavesdroppers.

Therefore, it would have been obvious for any one of ordinary skill in the art at the time of invention to modify the code generator (i.e. item 27 figure1) as taught by Groger to incorporate the variable code length as taught by KhHello for the benefit of providing a more secure system in that it allows the user to select different levels of security.

Regarding claim 20. Groger teaches the same code used but is silent with respect various input word lengths.

KhHello teaches a method and apparatus for user authentication wherein user selects code length (abstract, col. 10 lines 9-38) to provide different levels of security (abstract, col. 2 lines 46-49, col. 2 line 63 – col. 4 line 55, col. 8 lines 4-26). KhHello further discloses that the code length may be determined automatically by CPU or manually by person (col. 9 lines 24-53) providing an encryption algorithm that is highly secure against eavesdroppers.

Therefore, it would have been obvious for any one of ordinary skill in the art at the time of invention to modify the code generator (i.e. item 27 figure1) as taught by Groger to incorporate the variable code length as taught by KhHello for the benefit of

Art Unit: 2643

providing a more secure system in that it allows the user to select different levels of security.

Regarding claim 21. Groger does not elaborate on the size of encryption algorithm used with respect to the number of "bits". Khellos allows the user or CPU to select size of code word to provide different levels of security (see rejection listed for claim 11 directly above). Therefore, using 32 bits for lower security and 64 bits for higher security would have been an obvious measure to one of ordinary skill in the art at the time of invention.

Regarding claim 22. Groger does not elaborate on the size of the algorithm used with respect to "short" or "long". Khellos allows the user or CPU to select size of code word to provide different levels of security (see rejection listed for claim 11 directly above). Therefore, using smaller (i.e. short) word lengths for lower security and larger (i.e. long) word lengths for higher security would have been an obvious measure to one of ordinary skill in the art at the time of invention.

Regarding claim 23. Groger does not teach different output word lengths being used.

Khellos teaches a method and apparatus for user authentication wherein user selects code length (abstract, col. 10 lines 9-38) to provide different levels of security (abstract, col. 2 lines 46-49, col. 2 line 63 – col. 4 line 55, col. 8 lines 4-26). Khellos further discloses that the code length may be determined automatically by CPU or manually by person (col. 9 lines 24-53) providing an encryption algorithm that is highly secure against eavesdroppers.

Therefore, it would have been obvious for any one of ordinary skill in the art at the time of invention to modify the code generator (i.e. item 27 figure1) as taught by Groger to incorporate the variable code length as taught by Khello for the benefit of providing a more secure system in that it allows the user to select different levels of security.

Regarding claim 24. Applicant's have already acknowledged that Groger uses fixed length (i.e. a specified consistent result word length, see paper dated 3/7/05, second to last paragraph on page 18) but is silent with respect to using different input data word lengths.

Khello teaches a method and apparatus for user authentication wherein user selects code length (abstract, col. 10 lines 9-38) to provide different levels of security (abstract, col. 2 lines 46-49, col. 2 line 63 – col. 4 line 55, col. 8 lines 4-26). Khellos further discloses that the code length may be determined automatically by CPU or manually by person (col. 9 lines 24-53) providing an encryption algorithm that is highly secure against eavesdroppers.

Therefore, it would have been obvious for any one of ordinary skill in the art at the time of invention to modify the code generator (i.e. item 27 figure1) as taught by Groger to incorporate the variable code length as taught by Khello for the benefit of providing a more secure system in that it allows the user to select different levels of security.

Regarding claim 25. Groger does not explicitly show even or odd nibbles to form word length.

Khello teaches a method and apparatus for user authentication wherein user selects code length (abstract, col. 10 lines 9-38) to provide different levels of security (abstract, col. 2 lines 46-49, col. 2 line 63 – col. 4 line 55, col. 8 lines 4-26). Khellos further discloses that the code length may be determined automatically by CPU or manually by person (col. 9 lines 24-53) providing an encryption algorithm that is highly secure against eavesdroppers. Khello further discloses macros used to determine bit values to be used in the encoding algorithm (see figure 7b, col. 8 line 57 – col. 9 line 53, col. 10 lines 9-65).

Therefore, it would have been obvious for any one of ordinary skill in the art at the time of invention to modify the code generator (i.e. item 27 figure1) as taught by Groger to incorporate the variable code length as taught by Khello for the benefit of providing a more secure system in that it allows the user to select different levels of security.

Response to Arguments

2. Applicant's arguments with respect to claims 1 and new claims 11-25 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

3. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

---(6,148,053) Qzluturk is considered pertinent for also improving on prior art that uses fixed bit length (See Background and col. 3 line 65+) by using registers of different length (see at least col. 8 lines 7-8 and line 28).

---(6,834,341) Bahl et al is considered pertinent for offering different encryption algorithms having different input word lengths (see at least figure 6) allowing service providers the ability to tie a fee to the secret code, number of algorithms, and encryption level paid by users (col. 15 lines 30-43).

4. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Barry W. Taylor, telephone number (571) 272-7509, who is available Monday-Friday, 8am to 5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Curtis Kuntz, can be reached at (571) 272-7499. The central facsimile phone number for this group is **571-273-8300**.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group 2600 receptionist whose telephone number is (571) 272-2600, the 2600 Customer Service telephone number is (571) 272-2600.

Art Unit: 2643

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Centralized Delivery Policy: For patent related correspondence, hand carry deliveries must be made to the Customer Service Window (now located at the Randolph Building, 401 Dulany Street, Alexandria, VA 22314), and facsimile transmissions must be sent to the central fax number (571-273-8300).



Barry W. Taylor
Patent Examiner
Technology Center 2600
Art Unit 2643



CURTIS KUNTZ
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2600